PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07C 9/00, G07F 7/10 — A1

(11) International Publication Number: WO 98/13791

(43) International Publication Date: 2 April 1998 (02.04.98)

(21) International Application Number: PCT/US96/15509

(22) International Filing Date: 27 September 1996 (27.09.96)

(71) Applicant: WESTINGHOUSE ELECTRIC CORPORATION [US/US]; 11 Stanwix Street, Pittsburgh, PA 15222 (US).

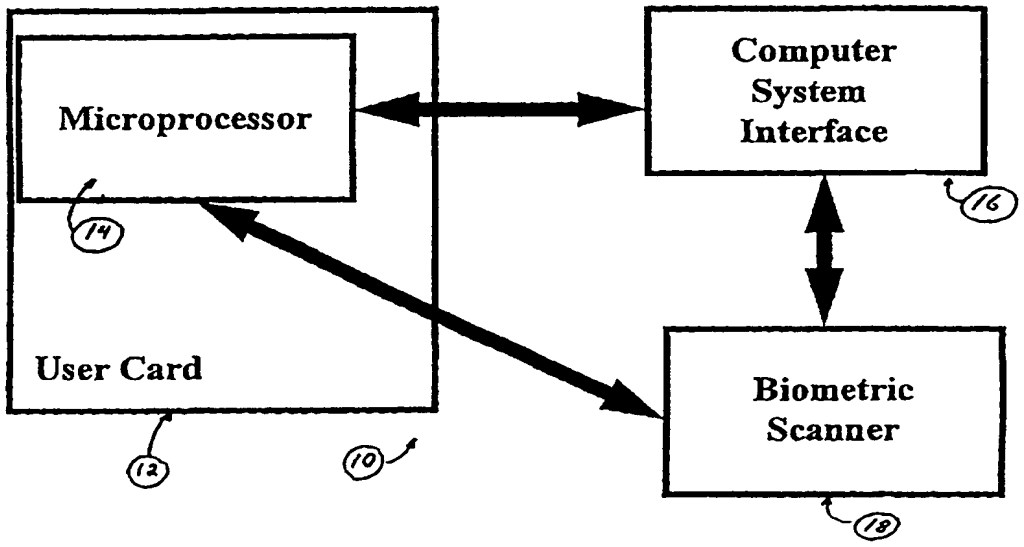
(72) Inventors: NELSON, Robert, A.; Route 1, Box 5555, Richland, WA 99352 (US). GRAMBIHLER, Anton, J.; 2008 Davison Avenue, Richland, WA 99352–2015 (US).

(74) Agents: STEVENS, Walter, S. et al.; Westinghouse Electric Corporation, 11 Stanwix Street, Pittsburgh, PA 15222 (US).

(81) Designated States: AU, CN, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: APPARATUS AND METHOD FOR PERSONAL IDENTIFICATION



(57) Abstract

There is provided by this invention a personal identification card for gaining access to controlled areas or computer systems having a microprocessor combined therein that has stored in its memory personal trait characteristics of the individual user. The microprocessor also has stored algorithms for comparing the personal trait characteristics stored in the card with personal trait characteristics inputted from an external device. Stored algorithms are used to update the personal stored traits. The microprocessor verifies the identity of the user of the card. A security system within the microprocessor protects the stored personal trait characteristics and restricts access to the card.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

APPARATUS AND METHOD FOR PERSONAL IDENTIFICATION

BACKGROUND OF THE INVENTION

Field of the Invention

The U.S. government has a paid-up license in this invention and the right in limited circumstances to require the patent owner to license others on reasonable terms as provided for by the terms of contract No. DE-AC06-87RL10930 award by the United States Department of Energy.

This invention relates generally to means for gaining access to controlled areas, but more particularly, to card systems for gaining access to secured buildings and facilities or to secured computer systems. This invention has broad applications in systems where bank cards, credit cards, or other types of plastic cards are used to gain access to automated financial transaction systems, and also to computer controlled systems where plastic cards are used for entering and leaving controlled buildings or other types of facilities. This invention also relates to applications where access to the information stored on the

card is restricted by a security system. Traditionally, these cards have a coded magnetic strip that allows the user to pass the strip through a reader which authorizes the user to gain access to the computer controlled system. Early versions of these basic systems allowed any holder of the card to gain entry to the system regardless of whether the holder was an authorized user or not. Later, these basic systems were supplemented with an additional identification means such as a PIN number or a password that had been previously stored in the computer memory. The holder of the card had to enter the identification into the system to prove he was an authorized user. These systems proved to be ineffective because the authorized user oftentimes forgot the password or PIN number and, in some cases, the PIN number and password were obtained by duress or theft or some other unauthorized means.

Then, systems were developed where a personal physical trait was actually stored on the card. These physical traits could be handwriting samples, photographs, or fingerprints. In these type systems, the personal trait that was stored on the identification card was also stored in a computer memory bank. When the user attempted to gain access to the secured system, the user would input the card to a reader or scanner that read the digitized personal information trait from the card and inputted it into the main computer memory bank. The main computer would then retrieve the stored information from its memory

bank and make a comparison of the information inputted from the reader. If the personal physical traits read on the card matched the personal traits stored in the main computer, then the user was authorized to gain access to the system. However, if there was not a match, then the user was denied access to the system. Such systems were disclosed in U.S. patent no. 5,214,699, issued May 25, 1993, to Midora Monroe, et al. See also U.S. patent no. 4,636,622, issued to Clemet Clark, on January 13, 1987. These systems were typical of systems that used identification cards to gain access to controlled areas or computer systems.

However, even these systems had major drawbacks. When personal identification traits and identities were stored in a centralized database where there were many, many users, databases of enormous size and expense were required. Inordinate delays were usually encountered when many users tried to gain access to the system simultaneously. They also require extensive communication between the remote access points and the central database.

Accordingly, other systems have been developed which require the user to place his personal identification card in a reader and then re-enter his personal identification trait in a real time on-line scanner. For instance, when a personal identification trait is a picture, a camera, located at the remote site, re-enters the user's picture into the system for comparison. Other systems may have

fingerprint scanners to read actual fingerprints or voice scanners compare actual voices with voiceprints stored on the identification cards. In these systems, the information read from the on-line scanner is fed to a main computer along with the information read from the identification card and a comparison is then made. If there is a match, then the user is allowed access to the system. These types of systems are disclosed in U.S. patent no. 4,993,068, issued to Gerald Piosenka, et al., and U.S. patent no. 5,229,764, issued to Noel Matchett, et al. See also U.S. patent no. 5,191,608, issued March 2, 1993, to Francois Geronimi wherein a secret code is coded in the microprocessor of the identification card which must be matched before the card is operational by the user.

However, these systems also have a major drawback. That is, they allow the personal trait information stored on the card to be read by an unknown or unfriendly computer. This type of technique compromises the security of the overall system.

It is an object of this invention to provide an identification card or smart card for use with an identification and access system wherein the personal identification trait stored on the smart card cannot be obtained by unauthorized users.

It is also an object to provide a system which may be used by numerous users without requiring a large centralized database. It is a still further object of this

invention to provide a multipurpose smart card which allows the user to gain access to a variety of different facilities or computer systems.

It is a further object of this invention to maintain secret information in the card that will not be released until the card holder proves his identity to the card. In all cases the identity verification takes place in the card.

Summary of the Invention

There is provided by this invention a portable device, preferably a personal identification card or smart card which contains a microprocessor with means for storing personal identification traits such as fingerprints, hand geometry, voiceprints, etc., in the memory of the microcomputer; biometric detection means such as a reader comprising a means for reading digitized data of personal identification traits template received from an external scanner; and means for comparing the inputted personal identification traits from the external scanner with the personal identification traits stored in programmable memory of the microprocessor. Upon obtaining a match of the stored personal identification traits and the scanned identification traits, the smart card allows access to a secured facility or computer system or the smart card itself. The smart card also contains security features which prevent any information from being inputted to the microprocessor from unauthorized computers.

Brief Description of the Drawings

Figure 1 is a simplified block diagram of the smart card interfacing with a computer system in accordance with the principles of this invention;

Figure 2 is a block diagram of the architecture of the microprocessor utilized on the smart card in accordance with the principles of this invention; and

Figure 3 is a flow chart illustrating the method of operation of the smart card in accordance with the principles of this invention.

Brief Description of Preferred Embodiment

There is shown in Figure 1 a personal identification system shown indicated generally at 10 that allows a user to gain access to controlled facilities or areas, or controlled computer system files in the smart card microprocessor. A person attempting to gain access to the system must have a user card 12 which may be a commonly used plastic card such as a credit card or other identification card which has contained therein a microprocessor generally referred to as 14. The user must connect the microprocessor to a computer system interface 16 by connecting serial communication, power, reset, and timing signal lines not shown but well known to those skilled in the art that allows the microprocessor and the computer system interface to communicate. The computer system interface is usually at a remote site so it is accessible to the user and is connected to a computer system not shown.

Also at the remote site is a biometric scanner 18 that is connected to the computer system interface 16 so that the microprocessor 14 and the biometric scanner 18 can pass information. The biometric scanner 18 may be any number of scanners well known in the art such as fingerprint scanners, voiceprint digitizers, hand geometry scanners, etc. Once the microprocessor 14 is connected to the computer system interface 16, the system will prompt the user to input information into the biometric scanner 18 for comparison in a manner hereinafter described.

Referring to Figure 2, there is shown a block diagram of the architecture of the microprocessor 14. Connected to the internal bus 20 are addressing logic circuits 22 and control and test registers 24 for the erasable, programmable read only memory (EPROM) or similar device 26 and the electrical erasable programmable read only memory (EEPROM) or similar device 28 which contains the templates for the biometric identification information and comparison and update codes. Also connected is an application read only memory (ROM) or similar device 30 and a data random access memory (RAM) 32. A CPU 34 is utilized to make the comparisons between the biometric template store and the biometric template input in a manner that will be hereinafter described. Finally, the microprocessor contains an input/output interface 36 and security logic control 38.

Although this system will work with any biometric identity verification trait, such as voiceprints or fingerprints, in the present invention hand geometry biometric information is used. When the card is issued to the user, a hand geometry template of the user is made, the information is digitized and inputted into the EEPROM 28. The microprocessor is programmed to make partial updates of the hand geometry template stored in the card. The template update accounts for subtle hand changes (e.g., fingernail growth and weight gain). The security logic circuits of the microprocessor protects the template and requires terminal verification before processing any International Organization for Standardization format command. The program maintains template integrity using an error detection code and an invalid access attempt count.

Figure 3 illustrates a flow chart that demonstrates the method of operation during identification of the user. When the card user inserts the card 12 into the computer system interface 16 and the microprocessor 14 is connected within the computer interface, the computer system interface challenges the user card to authenticate itself with a randomly generated security code. If the proper response is computed, the card is authenticated. If not, the computer system stops and the user is denied access. The system then prompts the user to place his hand in the hand scanner and a hand template is digitized by the hand

scanner 18. However, before this information is processed by the user card 12, the user card authenticates the terminal by challenging the terminal with a randomly generated security code. If the terminal security code is present, the template is made available to the user card 12. If it is not available, the system stops and the user is denied access. Once the hand template is available and the retry count has not been exceeded, the card requests that the hand template be sent to the card. The system denies access if the identity is unknown and the retry count is exceeded. The smart card then temporarily stores the hand template in the random access memory (RAM) 32 and retrieves the pre-stored hand template from the (EEPROM) 28. An algorithm stored for making a comparison is then used by the CPU 34 to compare the previously stored hand template with the hand template received from the scanner 18. The hand geometry comparison and update algorithm allows an update to be made to the stored template when a predetermined maximum score is made as a result of the comparison. The updated template then is stored and becomes the new stored template for comparisons for future entry attempts. When the computer system interface requests the results from the card, the holder is either identified and the user is granted access by the system or to the card, or the holder is not identified and the system denies access.

It can be readily seen that there is provided by this invention a novel, personal identification system wherein a personal identification card (smart card) has stored therein on a microprocessor system a template of biometric identification traits, such as hand geometry, which is protected from unauthorized or unfriendly computers by a security logic system. Once a computer system has been authenticated, then the smart card prompts the computer system to request a hand geometry scan which is digitized and sent to the smart card. Hand geometry algorithms and update algorithms stored in the smart card are compared with the hand geometry scan. Thus, every individual user of the system who has a smart card carries his template in his own microprocessor and relieves the main computer system from requiring excessive and expensive data storage space when there may be many thousands of potential users.

This invention provides a smart card where the biometric comparison occurs in the microprocessor of the smart card.

Although there has been illustrated and described specific detail and structure of operation, it is clearly understood that the same were merely for purposes of illustration and that changes and modifications may be readily made therein by those skilled in the art without departing from the spirit and the scope of this invention.

What is claimed is:

1. A personal identification system for controlling access to a protected system, comprising:

a) a portable device containing a microprocessor means disposed to be inputted into a computer system interface means for controlling access to the secure area or computer system;

b) biometric reader means connected to the computer system interface means for detecting personal trait characteristics of an individual seeking access and producing a digitized output of the personal trait characteristics;

c) programmable memory means within the microprocessor means for storing previously recorded biometric personal trait characteristics;

d) comparative means within the microprocessor means for comparing the previously stored personal trait characteristics in the programmable memory means with the output of the biometric detection means for verifying the identity of the individual seeking access;

e) output means within the microprocessor means for producing an output signal resulting from the comparison made in the comparative means to the computer interface means for enabling or disabling access of the individual to the secured areas or computer system; and

f) security means within the microprocessor means wherein access to the personal trait characteristics is protected and restricted.

2. A personal identification system as recited in Claim 1 wherein the portable device is a card.

3. A personal identification system as recited in Claim 2 wherein the card is plastic.

4. A personal identification system as recited in Claim 3 wherein the biometric detection means is comprised of a scanner for digitizing the hand geometry of the individual seeking access.

5. A personal identification system as recited in Claim 4 wherein the biometric detection means is a receiver for digitizing voiceprints of the individual seeking access.

6. A personal identification system as recited in Claim 5 wherein the programmable memory means updates the previously recorded personal trait characteristics with the digitized output of the biometric detection means.

7. A personal identification system as recited in Claim 6 wherein the protected system is a controlled area or facility.

8. A personal identification system as recited in Claim 7 wherein the protected system is a computer system.

9. A portable device for accessing a protected system by the user, comprising a microprocessor wherein the microprocessor means is further comprised of:

a) a programmable memory means for storing previously recorded personal trait characteristics;

b) means for storing personal trait comparison algorithms and personal trait update algorithms;

c) computing means for utilizing the personal trait comparison algorithms for comparing personal trait characteristics inputted into the microprocessor means with the previously recorded personal trait characteristics stored in the programmable memory means;

d) update means for updating the personal trait characteristics previously recorded stored in the programmable memory means with the personal trait characteristics inputted into the microprocessor means;

e) output means for producing an output signal based upon the comparison made in the computing means between the personal trait characteristics previously recorded and a personal trait characteristic inputted into the microprocessor means to verify the identity of the user; and

f) security means within the microprocessor means wherein access to the personal trait characteristics is protected and restricted.

10. A method of controlling access to a protected system by an individual, consisting of the steps of:

providing portable storage means for storing personal trait characteristics of an individual;

verifying the portable device upon input to the protected system;

verifying the protected system by the portable device;

measuring personal trait characteristics of the individual seeking access and inputting the personal trait characteristics into the portable device;

comparing the personal trait characteristics inputted into the portable device with the personal trait characteristics previously stored in the portable device for determining the identity of the user; and

signaling the protected system to enable or disable access by the individual based upon the comparisons made.

11. A method for controlling access to a protected system as recited in Claim 10 further comprising a step of updating the personal trait characteristics stored in the portable device by the personal trait characteristics measured and inputted into the portable device.

12. A method for controlling access to a protected system as recited in Claim 11 wherein the portable device is comprised of a card having a microprocessor attached thereto.

13. A method for controlling access to a protected system as recited in Claim 12 wherein the card is plastic.

14. A method for controlling access to a protected system as recited in Claim 13 wherein the protected system is a secure area or facility.

15. A method for controlling access to a protected system as recited in Claim 14 wherein the protected system is a computer system.

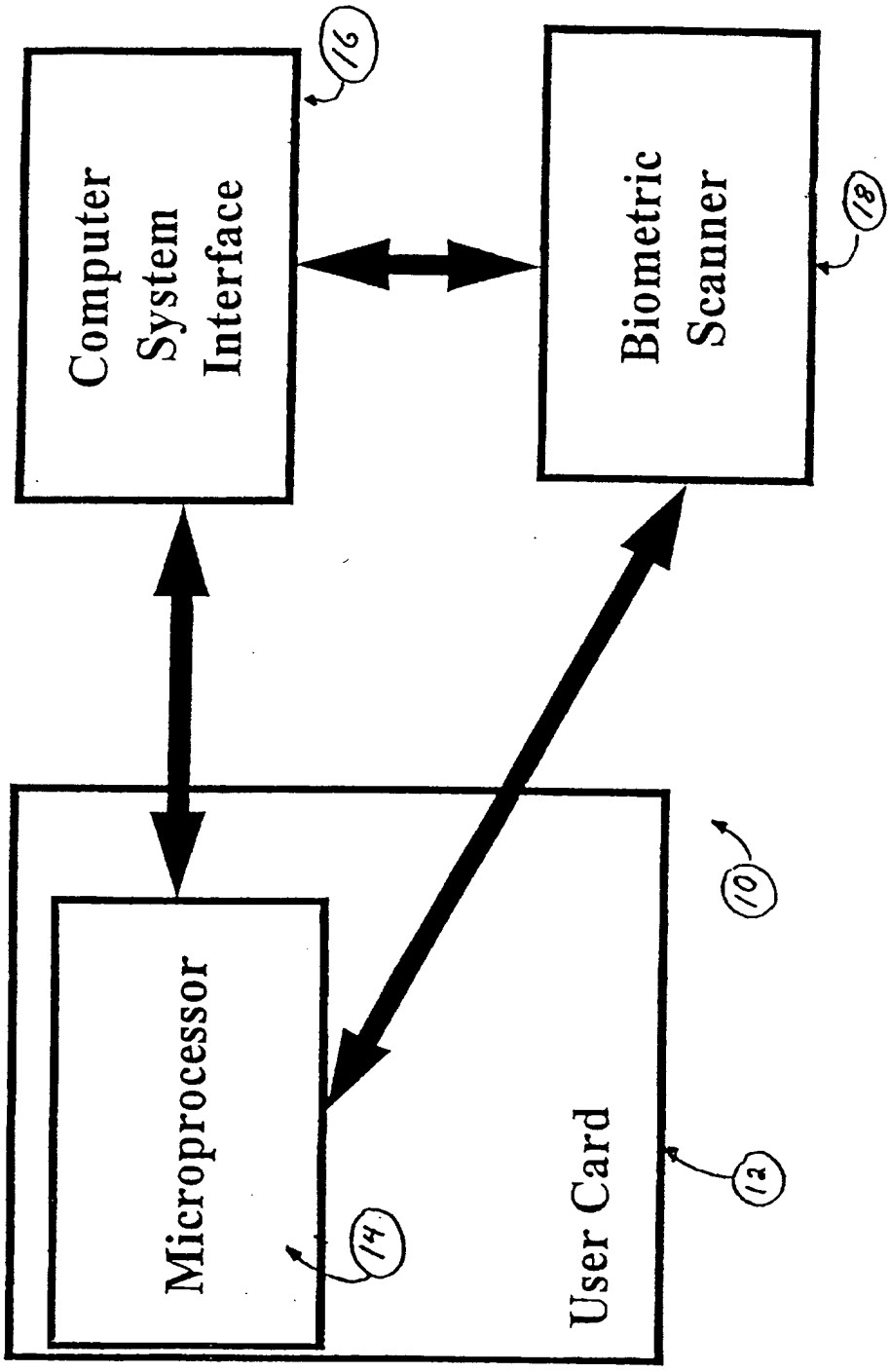

Computer System Interface
16
Biometric Scanner
18
Microprocessor
14
User Card
12
10

Figure 1

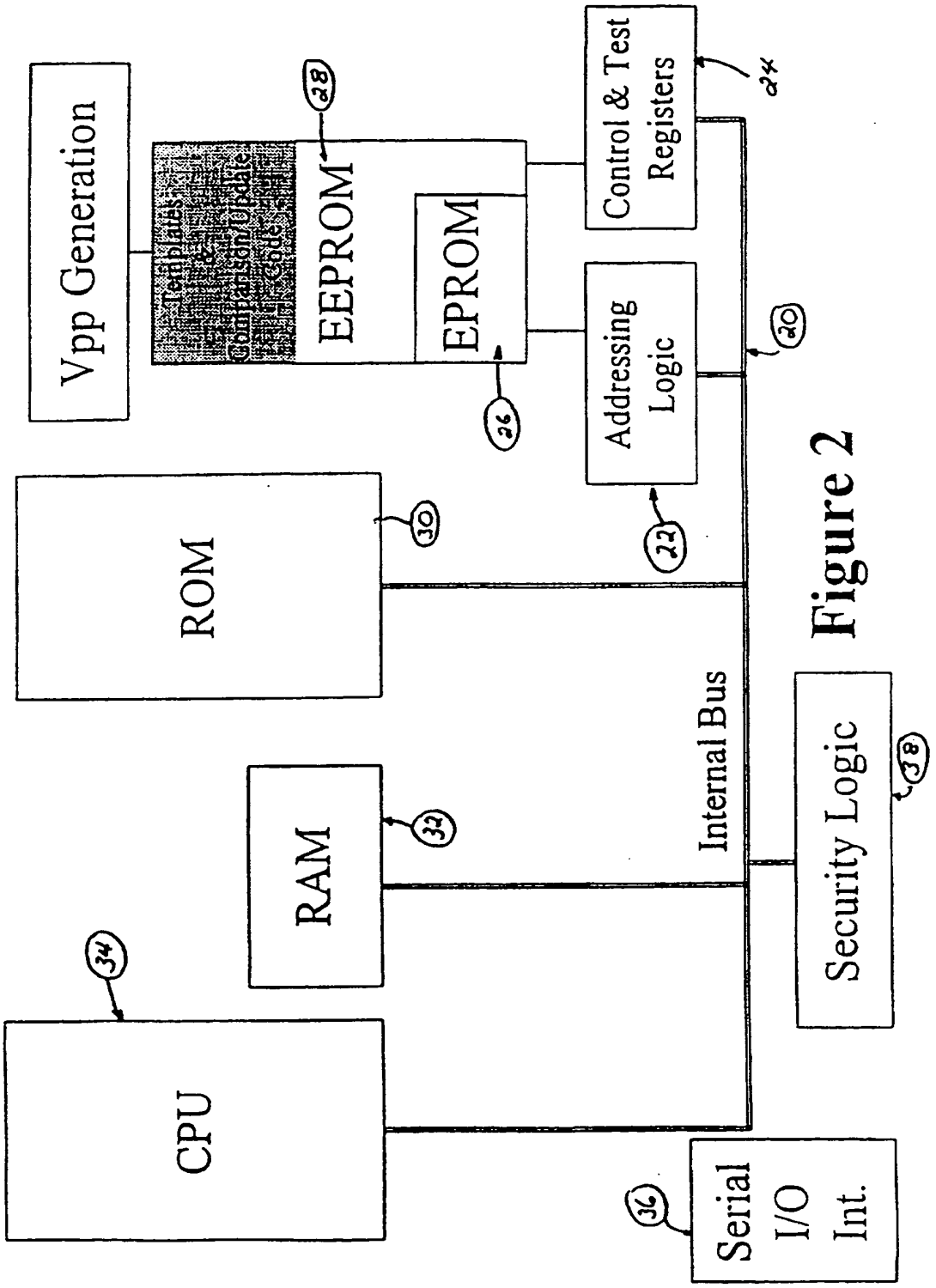

Vpp Generation
Test Data & Comparison/Update Code
28
EEPROM
EPROM
26
Control & Test Registers
24
Addressing Logic
20
22
ROM
30
RAM
32
Internal Bus
Security Logic
38
CPU
34
Serial I/O Int.
36

Figure 2

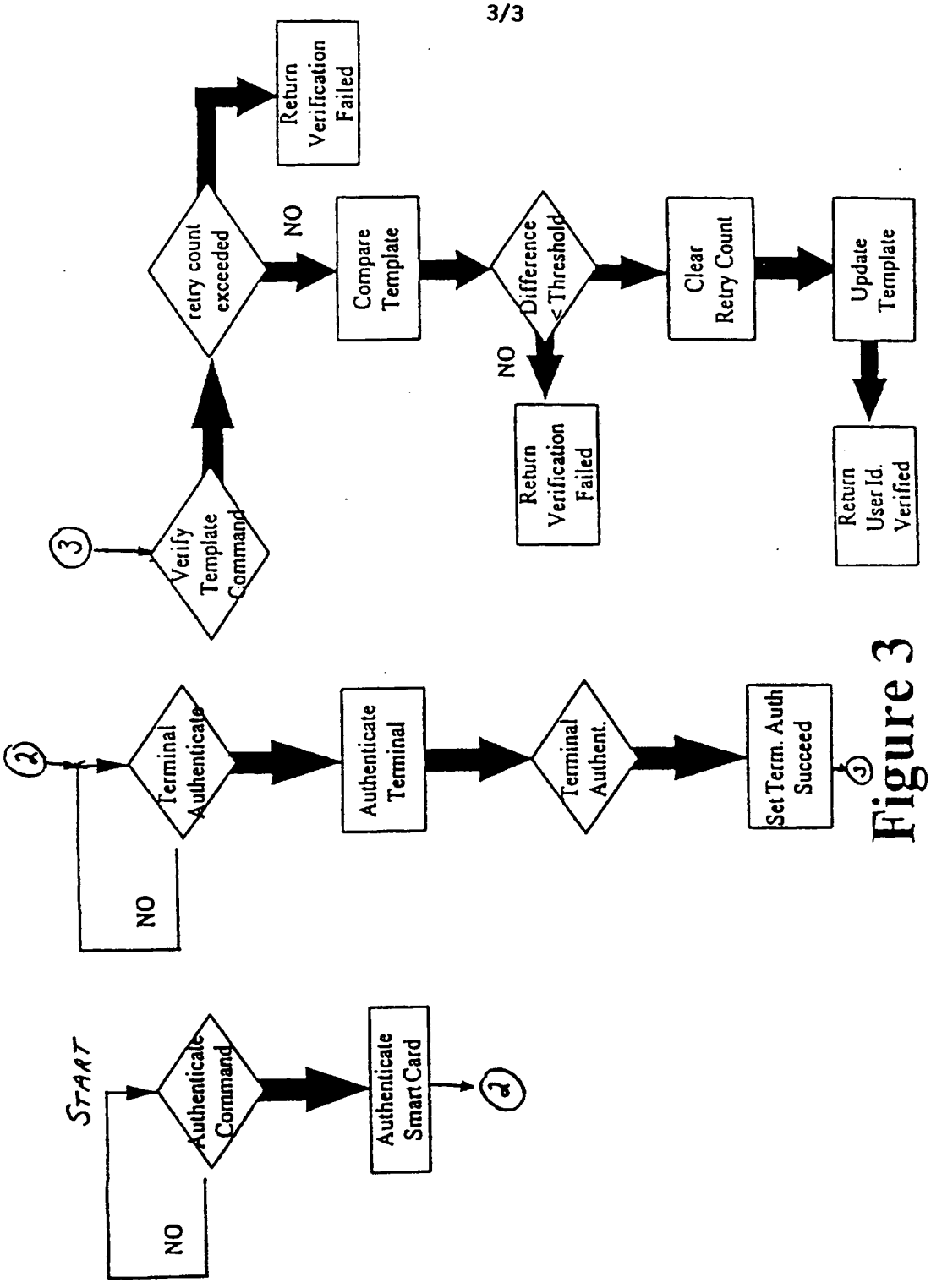

START
Authenticate Command
NO
Authenticate Smart Card
2
2
Terminal Authenticate
NO
Authenticate Terminal
Terminal Authent.
Set Term. Auth Succeed
3
3
Verify Template Command
retry count exceeded
NO
Return Verification Failed
Compare Template
Difference < Threshold
NO
Return Verification Failed
Clear Retry Count
Update Template
Return User Id. Verified

Figure 3

INTERNATIONAL SEARCH REPORT

Inte ɔnal Application No
PCT/US 96/15509

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	GB 2 204 971 A (GEN ELECTRIC CO PLC) 23 November 1988 see page 2, line 26 - page 6, line 19; figures	1-15
Y	GB 2 181 582 A (BLACKWELL VICTOR CAMPBELL) 23 April 1987 see abstract; claims; figures see page 1, line 66 - page 2, line 28 see page 2, line 89 - page 3, line 99	1-15
A	EP 0 197 535 A (SIEMENS AG) 15 October 1986 see column 2, line 1 - column 3, line 53; figures	1-3,9-15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
12 June 1997	02. 07. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Meyl, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 96/15509

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 615 984 A (TOSHIBA) 2 December 1988 see abstract; claims; figures	1-3,5-7, 9-14
A	GB 2 171 828 A (MITSUBISHI ELECTRIC CORP) 3 September 1986 see abstract; claims; figures see page 1, line 11 - line 86 see page 2, line 101 - page 3, line 70	1-3,9,10
A	WO 82 03286 A (LOEFBERG BO) 30 September 1982 see abstract; claims; figures see page 5, line 23 - page 7, line 12	1,2,7-10
A	PATENT ABSTRACTS OF JAPAN vol. 016, no. 085 (P-1319), 28 February 1992 & JP 03 269692 A (HITACHI LTD), 2 December 1991, see abstract	1,2,9,10
A	EP 0 393 784 A (NEDAP NV) 24 October 1990 see abstract; claims; figures see column 3, line 2 - column 4, line 31	1,2,9,10
A	EP 0 271 835 A (HITACHI LTD) 22 June 1988 see abstract; claims; figures see column 2, line 34 - column 4, line 9	1,2, 5-10, 12-15

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...information on patent family members

Inter nal Application No
PCT/US 96/15509

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2204971 A	23-11-88	NONE	
GB 2181582 A	23-04-87	AU 6476786 A	05-05-87
		EP 0241504 A	21-10-87
		WO 8702491 A	23-04-87
EP 0197535 A	15-10-86	NONE	
FR 2615984 A	02-12-88	JP 7121630 B	25-12-95
		JP 63299996 A	07-12-88
		US 4851654 A	25-07-89
GB 2171828 A	03-09-86	JP 61199162 A	03-09-86
		JP 62031471 A	10-02-87
		FR 2578340 A	05-09-86
		US 5144680 A	01-09-92
WO 8203286 A	30-09-82	SE 425704 B	25-10-82
		AU 8273682 A	06-10-82
		EP 0085680 A	17-08-83
		SE 8101707 A	19-09-82
		US 4582985 A	15-04-86
EP 0393784 A	24-10-90	NL 8900949 A	16-11-90
		CA 2014687 A	17-10-90
EP 0271835 A	22-06-88	JP 7095240 B	11-10-95
		JP 63155194 A	28-06-88
		DE 3784872 A	22-04-93